FORTINET
High Performance Network Security

FortiGate - RSSO with Windows Server 2012 R2 and NPS

VERSION 5.2.4

FORTINET DOCUMENT LIBRARY

http://docs.fortinet.com

FORTINET VIDEO GUIDE

http://video.fortinet.com

FORTINET BLOG

https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT

https://support.fortinet.com

http://cookbook.fortinet.com/how-to-work-with-fortinet-support/

FORTIGATE COOKBOOK

http://cookbook.fortinet.com

FORTINET TRAINING SERVICES

http://www.fortinet.com/training

FORTIGUARD CENTER

http://www.fortiguard.com

END USER LICENSE AGREEMENT

http://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK

Email: techdocs@fortinet.com

28/01/2016

FortiGate - RSSO with Windows Server 2012 R2 and NPS

Version 2.2

TABLE OF CONTENTS

Change Log

Date	Change Description
2016-01-28	Initial release.

Introduction

The purpose of this guide is to provide a known working configuration of RADIUS single sign-on using the following component

- FortiGate (FortiOS 5.2.4)
- Windows Server 2012 R2 with Network Policy Server
- FortiAP (v5.-build0245)
- Windows 7 SP1 laptop supporting 802.1X wireless authentication

This guide assumes that you have a working wireless authentication infrastructure, that Virtual Domains are not enabled on the FortiGate, and that Certificate Services are installed on the Network Policy Server (NPS). A Root CA is required because the CA public key is an integral part of 802.1x and will not work without it.

Lastly, this guide is intended for small to medium IT environments. Some medium-sized and certainly enterprise-sized environments should use a FortiAuthenticator in place of the FortiGate (with regards to RADIUS and authentication) due to the better authentication scalability and flexibility that product offers.

Audience

This guide is written for network and security administrators that have intermediate expertise in the following domains:

- Microsoft Server 2012 and Network Policy (NPS) Server administration
- Configuring Protected EAP with MS-CHAPv2
- Windows 7 administration
- FortiOS administration
- Wireless Access Point (AP) configuration

RADIUS Overview

Clarification of Terms

'RADIUS Single Sign-On' or RSSO – A FortiOS feature which uses RADIUS accounting start/interim/stop messages to extract information including username, IP Address and group memberships. The group parameter (Class attribute) is used to match a local Fortigate RSSO Group containing the string we expect to receive from the RADIUS peer. RSSO does not lookup incoming user accounts against LDAP or any other authorization backend information, and does not therefore know what groups a given AD user is a member of. Hence an admin will need to manage totally separate identity groups versus FSSO even if the users are the same.

'RADIUS Accounting' – A FortiAuthenticator feature which also uses RADIUS accounting start/interim/stop messages to extract information including username, IP Address and group memberships. The FortiAuthenticator then queries an LDAP backend for a given username and extracts all group memberships for which that user is a member. The FortiAuthenticator can then create standard FSSO Groups with that information allowing the same group information within a FortiOS policy to remain identical to FSSO/AD. The benefit is it provides one set of unified FSSO Groups for identity based rules.

In summary of the above, RSSO does not equate to RADIUS Accounting as most environments ideally want to be using RADIUS Accounting, and thus FortiAuthenticator, to avoid the complexity surrounding the management of two separate types of group identity. 'RADIUS Accounting Proxy' – A FortiAuthenticator feature that proxies RADIUS accounting records, modifies them if required, and replicates them to the multiple subscribing endpoints (RADIUS peers) as needed.

RSSO Use Case

In a traditional Microsoft Active Directory wired environment, users log into their machines and have their logon attempt validated by the domain controller. The domain controller security event log is polled for that logon event and that information is sent to the FortiGate to record the IP address, username and group information associated with that event. Typically, that IP address is assigned to that host (either via a static IP address or an extended DHCP lease time) that does not change. However, as wireless is being adopted more frequently in the enterprise environment for both company owned and Bring Your Own Device (BYOD) assets, this traditional method of single sign-on is not as effective.

When a host has both a wired and wireless connection available to them, it typically makes the authentication request via its more preferred interface (typically wired). The IP address associated with that interface is what is sent to the FortiGate. However, when a user disconnects from the wired connection (i.e. via undocking the laptop, link failure from the network card, etc.), the FortiGate has no knowledge of the wireless interface IP address and therefore, the user is no longer authenticated to the firewall. The user could go through the cumbersome task of signing out of their desktop and re-signing in (to make the authentication request from their wireless IP), however this is not preferred.

RSSO bridges this gap by harnessing the wireless authentication (802.1X) request from the RADIUS server authenticating that request via RADIUS accounting. Essentially RADIUS accounting captures valid logon information which identifies when a valid session starts and ends. In this deployment, the FortiGate wireless

controller forwards its accounting packets to the RADIUS server who then injects those packets to the RSSO agent listening on the FortiGate.

RADIUS Connectivity Flow

1. Wifi user connects to an AP SSID, the AP sends the username and password to RADIUS server.
2. RADIUS server sends Access-Accept back to the AP confirming the username and password are accepted.
3. AP allows the host to continue the wireless connection and assigns an IP Address via DHCP to the user.
4. Access point sends Accounting request message back to RADIUS including Framed-IP-Address.
5. RADIUS forwards Accounting request including Username, Framed-IP-Address, and Class attribute value to FortiGate.
6. Fortigate inserts Username, Class attribute value, and IP Address into its database.
7. FortiGate matches the Class attribute value to and RSSO group value, which in turn is used in and Identity Based Policy to control access.
8. User can now access network resources as per policy with a single sign-on, without the need to re-authenticate to the FortiGate.

What is Protected EAP

Protected EAP (PEAP) with MS-CHAP v2 is an EAP type that this design guide uses which is more easily deployed than Extensible Authentication Protocol with Transport Level Security (EAP-TLS) or PEAP-TLS because user authentication is accomplished by using password-based credentials (an Active Directory username and password) instead of digital certificates or smart cards. Only servers running Network Policy Server (NPS) or PEAP-MS-CHAP v2 are required to have a certificate.

This next part is optional, the administrator can design to the solution to not use ‘Server Validation’ however that would not be advised. When using Server Validation successful PEAP-MS-CHAP v2 authentication requires that the client trust the NPS server after examining the server certificate.

For the client to trust the NPS server, the certification authority (CA) that issued the server certificate must have its own different certificate in the Trusted Root Certification Authorities certificate store on the client computer.

The server certificate used by NPS can be issued by your organization’s private trusted root CA deployed on your network, or by a public CA, such as VeriSign or Thawte, that is already trusted by the client computer.

What is Single Sign-On Overview

Single sign-on (SSO) is a property of access control of multiple related, but independent software systems. With this property a user logs in once and gains access to all systems without being prompted to log in again at each of them (Reference: https://en.wikipedia.org/wiki/Single_sign-on).

In the case of FortiGate, it means harnessing a previous authentication attempt (i.e. an Active Directory domain user account, 802.1X wireless authentication, etc.) to reconcile IP addresses to a username as well as assign privilege to a user without prompting authentication from the client.

FortiGate Configuration

Excluding the FortiAP profile (outside the scope of this guide, but briefly described below) there are three main components required to support RSSO functionality. Those components are specific to the FortiGate, FortiAP, and Windows Server 2012 R2 NPS. This guide also includes an optional step of Server Validation that the client performs against the RADIUS server as described in the PEAP section above.

Wireless LAN Controller Overview

The FortiGate acts as the Wireless LAN Controller (WLC) for the FortiAP and uses a CAPWAP protocol listener to establish a management tunnel between the two. The FortiAP is either on same local subnet as the CAPWAP listener and broadcasts to the WLC, or the FortiAP is pre-configured with all the IP Addressing details before being sent to a remote location and uses its default gateway to Unicasts to the WLC to establish the tunnel.

Finally, once the ForitAP is authorized and a CAPWAP tunnel established, the WLC sends a Profile to the FortiAP including an SSID that instructs the FortiAP to use WPA Enterprise Security Mode with RADIUS as an authentication method for clients wishing to connect. The client then uses configuration similar to what is shown below to match the SSID requirements.

- Security – WPA2 Enterprise (802.1x EAP)
- EAP Method – PEAP
- Phase 2 Authentication – MSCHAPV2
- Root CA Certificate from NPS (optional)
- Username and Password

The main configuration components we will be working with are shown below:

1. RSSO Accounting Listener which listens on port 1813 for accounting packets
2. RADIUS Accounting and FortiGate RADIUS server
3. RSSO Group creation based on attribute sent in RADIUS accounting packets

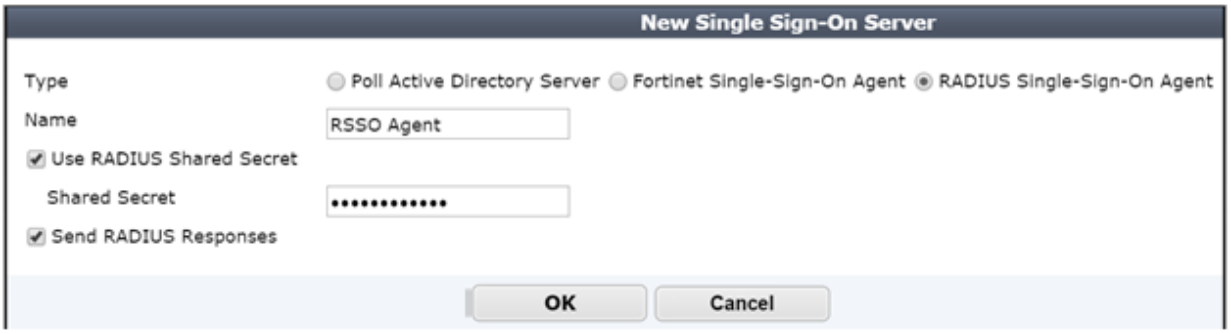
At the conclusion of this section, the FortiGate will be listening for accounting messages from an external RADIUS server (Windows NPS in this case) and sending accounting packets when the FortiAP authenticates a user via 802.1X. There will also be a new user RSSO group that can be used to create identity based policies on the FortiGate.

RADIUS Accounting Listener

1. Log into the FortiGate with Administrator credentials.
2. Click on **User & Device > Authentication > Single Sign-On**.
3. Click **Create New**.
   Note: The existing Single Sign-On entries are not used for the purposes of this document.
4. Under the **New Single Sign-On Server** section:

a. Select **RADIUS Single-Sign-On Agent**.
b. Check **Use RADIUS Shared Secret**.
c. Populate the **Shared Secret** with that of the NPS.
d. Check **Send RADIUS Responses**.
e. Click **OK**.

Screenshot of New Single Sign-On Server configuration page



6. Connect to the CLI of the FortiGate with an administrative user.
7. Modify the "RSSO Agent" configuration with the RADIUS attribute that will be used from the AP to denote username:

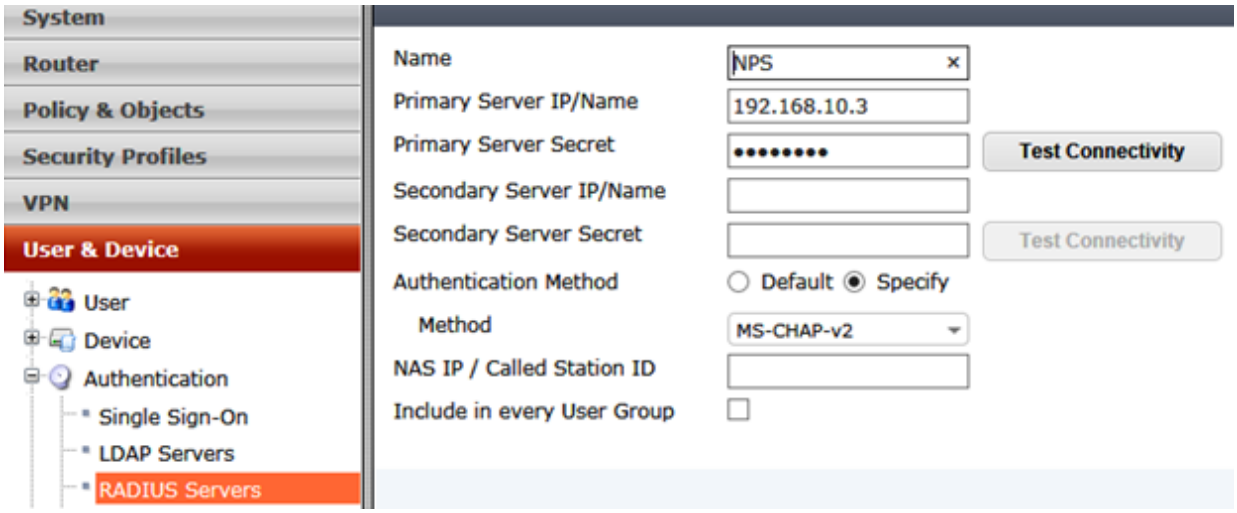
```
config user RADIUS
   edit "RSSO Agent"
      set rsso enable
      set rsso-RADIUS-response enable
      set rsso-validate-request-secret enable
      set rsso-secret ENC
uq7eceRhIZ1qkPIpmdZq1rfZabcJu/E6LH4aZqkgRZO8bxkEZoFh5LeRfVr4NrTk66SxS5gYHjcn/owXrRXVCtlWET
+i05cRi+q/APdtgfWUSYLNWwzyg1esGanr2tnPg/ew3zTwq95PCItH5GdH6Zan9ARzv0mcbZ6zVOYlrwJ+EDPn+UN2
9x5+tb/9pLc7McNhjQ==
      set rsso-endpoint-attributeUser-Name
      set rsso-context-timeout0 (this value controls the auth time in seconds)
      set rsso-flush-ip-sessionenable
   next
end
```

Note: The RADIUS attribute used by FortiAP to denote user is "User-Name". Please check your AP vendor's specific documentation to find out their corresponding attribute for this field in their RADIUS accounting packets.

The rsso-context-timeout can be used to clear authentications after x (0 is never time out) number of seconds. This works together with the DHCP Lease Time and rsso-flush-ip-session, adjust as required.

RADIUS Accounting from WLC

1. Create a new RADIUS server peer (which needs matching peer config in NPS) as shown below.
2. On the interface pointing towards the NPS, click 'Edit' on the gui for that interface and select 'Listen for RADIUS Accounting Messages'. For reference in this document, 192.168.0.1 is the FGT port with the 'RADIUS-ACCT' listener.



3. Log into the CLI of the FortiGate.
4. Modify the existing RADIUS server used for 802.1X authentication to send accounting packets for any connection that uses that server:

```
config user RADIUS
   edit "NPS"
      set server "192.168.10.3"
      set secret <shared secret with NPS>
      set auth-type ms_chap_v2
      set source-ip 192.168.0.1(use FGT interface to simplify administration)
         config accounting-server
            edit 1
               set statusenable
               set server"192.168.10.3" (NPS server)
               set secret<shared secret with NPS>
               set source-ip 192.168.0.1(use FGT interface to simplify
                  administration)
            next
         end
   next
end
```

Note: Accounting packets will now be sent to port 1813 of the NPS server.

RADIUS Group Matching

The identity based policies can be used to provide access through the FortiGate via the attribute matched by this group.

1. Log into the WebGUI with Administrative credentials.
2. Click on **User & Device > User > User Groups**.
3. Click **Create New**.

Screenshot of User Groups

4. In the **Edit User Group** page:
   a. Type in a **Name** for the user group.
   b. Select **RADIUS Single Sign-On (RSSO)** as type.
   c. Type in **RADIUS Attribute Value** for the group. This is the value NPS will send (in Hex) and the FGT will use that value to verify successful user authentication for later Identity-based Policies.
   d. Click **OK**.

Screenshot of Edit User Group page

Microsoft Network Policy Server (NPS)

The Microsoft NPS provides the authentication and proxy accounting functionality in this environment. When a user provides login details to via the AP, the WLC will send those details to the NPS in order to verify the username and password against Active Directory. The NPS will also respond to the WLC with information including a RADIUS Class attribute that contains the specific value (see Figure 6) which relates to the FortiGate RSSO Group. This attribute can be used to create identity based policies which govern the access of that user based on RSSO group membership rather than IP address alone.

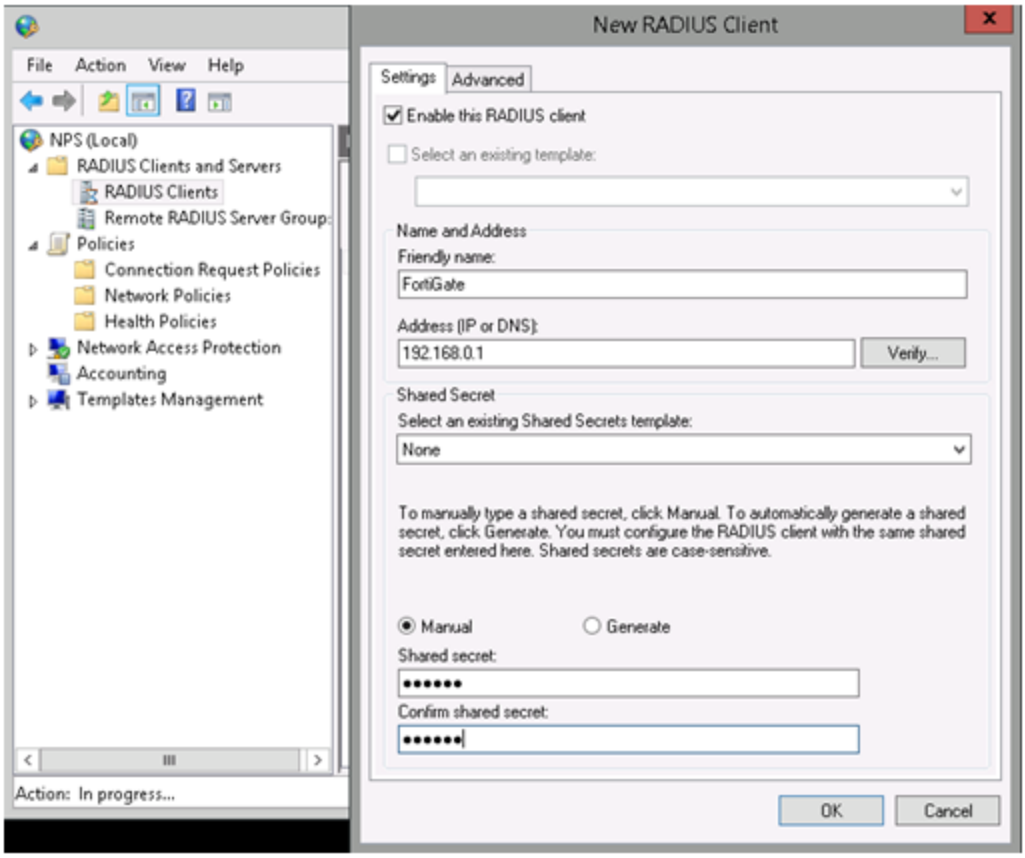
At the end of this section, the NPS will be configured to:

1. Authenticate users and return the correct attribute based on Windows group membership.
2. Forward RADIUS accounting packets to the FortiGate for RSSO.

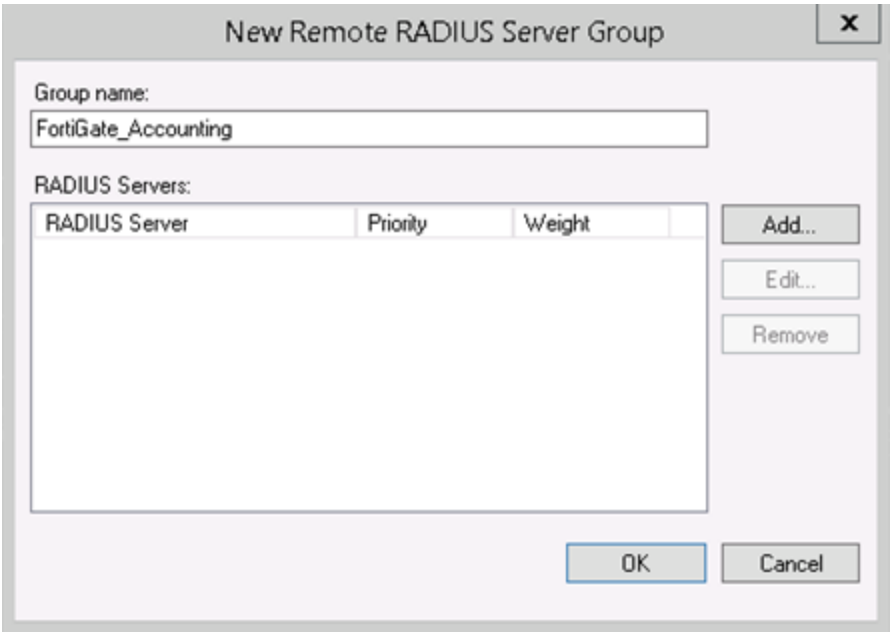
Client and Remote RADIUS Server Group

1. In the **Network Policy Server**, click **NPS (Local) > RADIUS Clients and Servers**.
2. Right-click **RADIUS Clients**, select **New**, and enter **Friendly name**, **IP Address**, and **Shared Secret** which must match the FortiGate RSSO_Agent shared secret entered in a previous step.

Screenshot of Edit User Group page

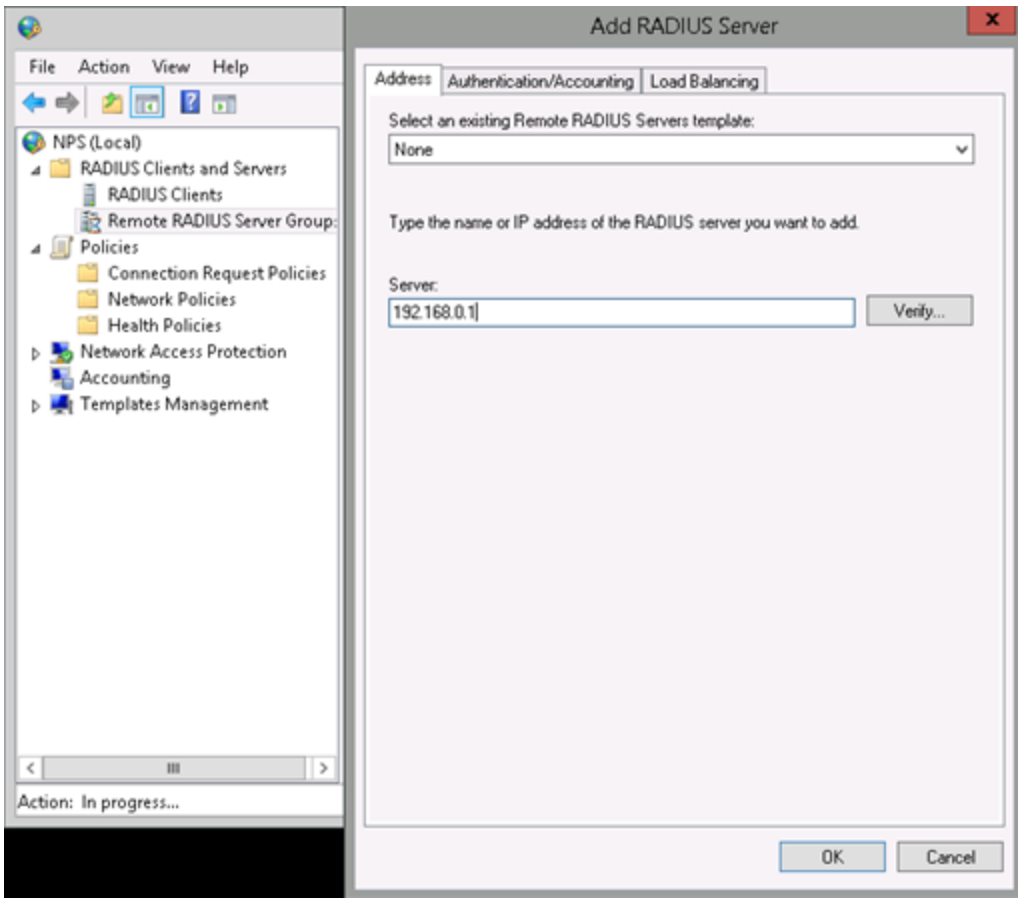


3. Right-click **Remote RADIUS Server Groups**, select **New**, and enter the group name and click **Add**.



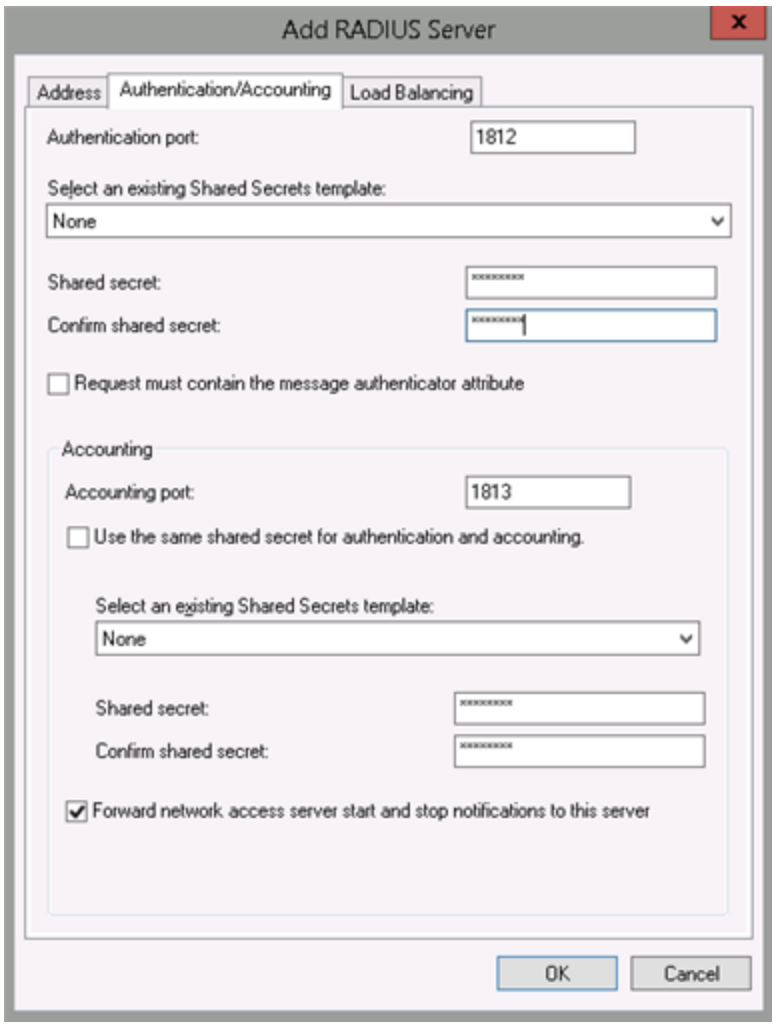
4. Use the FortiGate interface that was configured to **Listen for RADIUS Accounting Messages** from a previous step and enter that IP address.

Screenshot of NPS RADIUS Server Group



5. Click on the **Authentication/Accounting** tab:
   a. Un-check **Use the same shared secret for authentication and accounting**.
   b. Type in the accounting **Shared Secret** which must match the FortiGate RSSO_Agent entered previously.
   c. Check **Forward network access server start and stop notifications to this server**.
   d. Click **OK**.

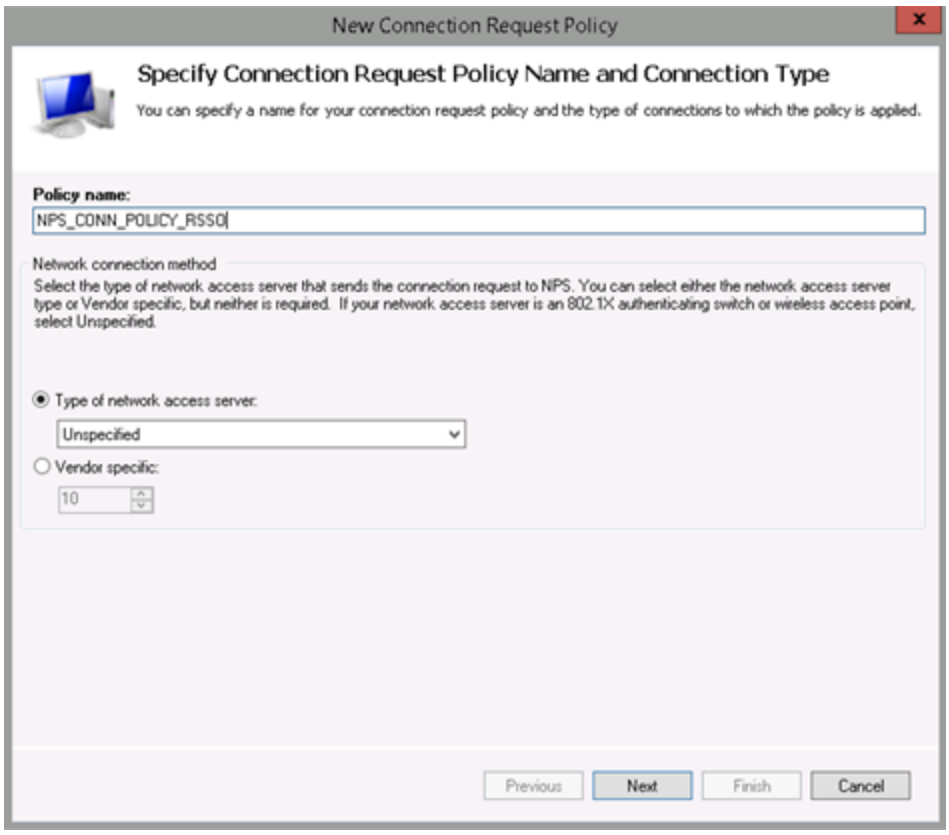
Screenshot of RADIUS Server Authentication/Accounting dialog box



Connection Request Policy

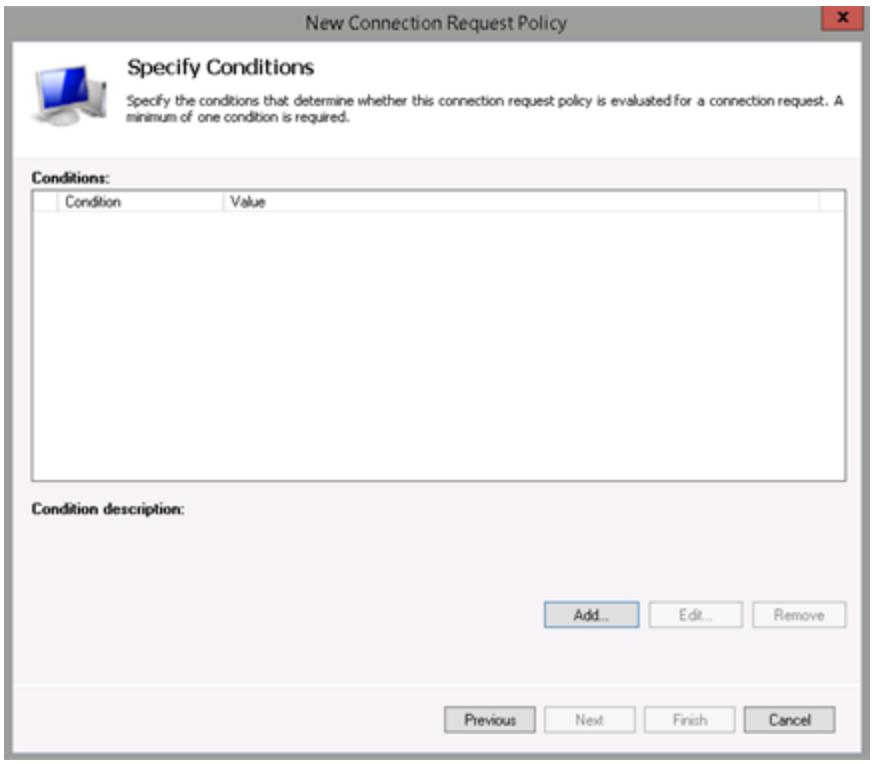
1. In the Network Policy Server:
   a. Right-click **Policies > Connection Request Policy**.
   b. Select **New** (make sure to use a descriptive name that will stand out in the Server Security Event Log e.g. *NPS_CONN_POLICY_RSSO*).
   Provide a **Policy Name** and click **Next**.

Screenshot of New Connection Request Policy Wizard



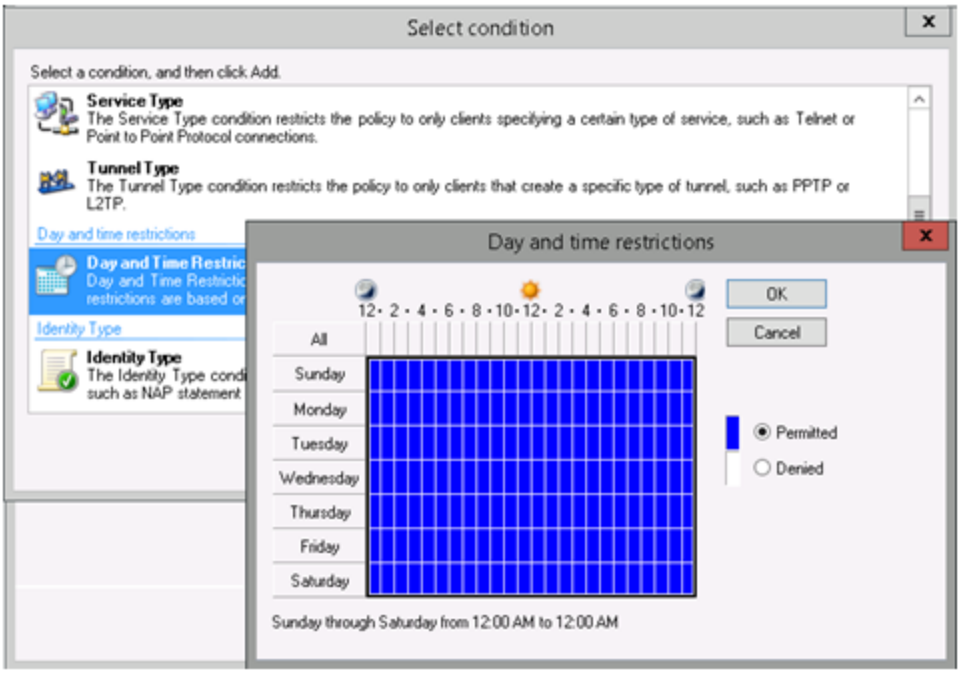
2. Under the Conditions page, click **Add**.

Screenshot of Specify Conditions dialog



3. Select **Day and Time Restrictions** and choose day/time and required.
   a. Click **Add** and **OK**.
   b. In the Select Conditions dialog:

Screenshot of Select Condition for Day and Time Restriction dialog

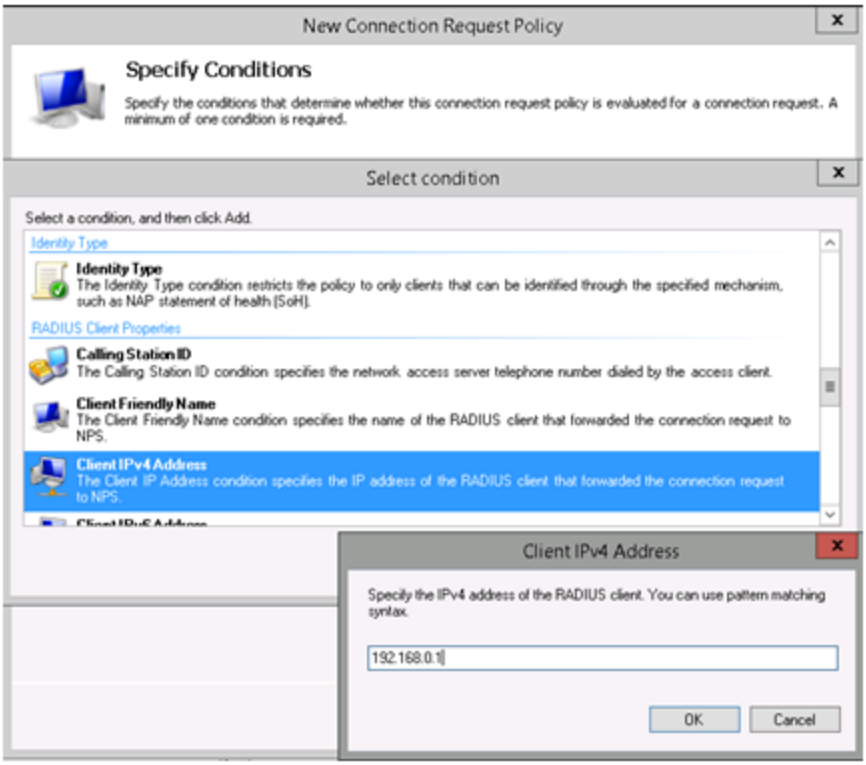


c. Click **Add**.

d. Select **Client IPv4 Address** (adding this more predictably binds this connect policy to the network policy in the next step).

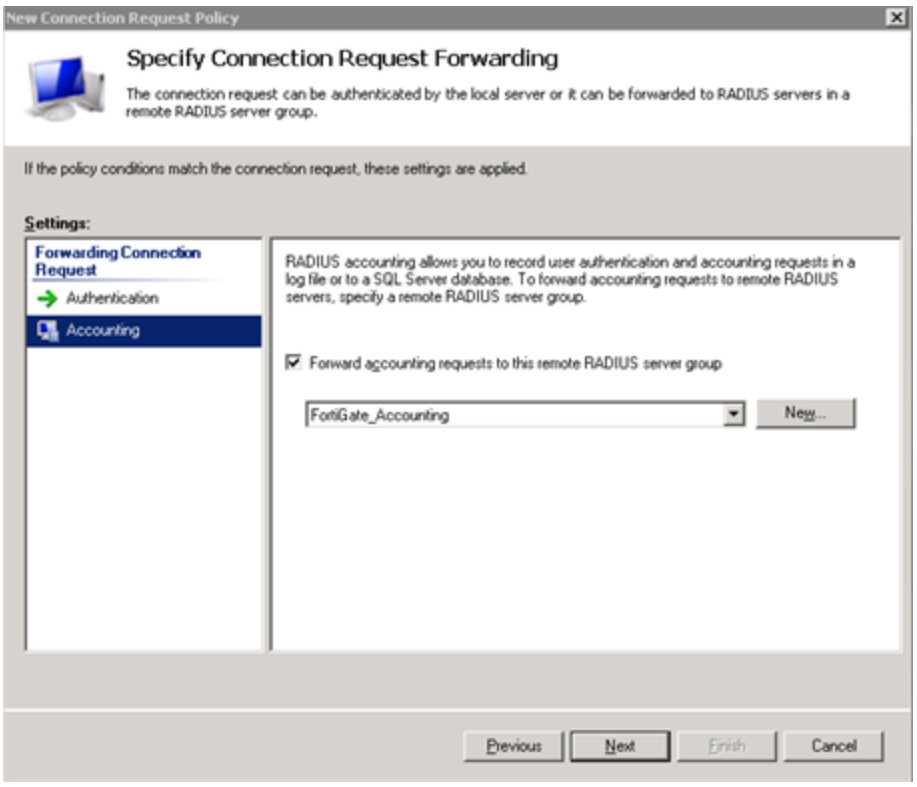
e. Click **Add** and **OK**.

Screenshot of Select Condition for Client IPv4 Address dialog



4. Click **Next**.
5. In the **Specify Connection Request Forwarding** dialog:
   a. Leave Authentication as default **Authenticate requests on this server**.
   b. Click **Accounting**.
   c. Check the **Forward accounting requests to this remote RADIUS server group**.
   d. Select the FortiGate accounting group created from the drop down box.
   e. Click **Next**.

Screenshot of Specify Connection Request Forwarding dialog

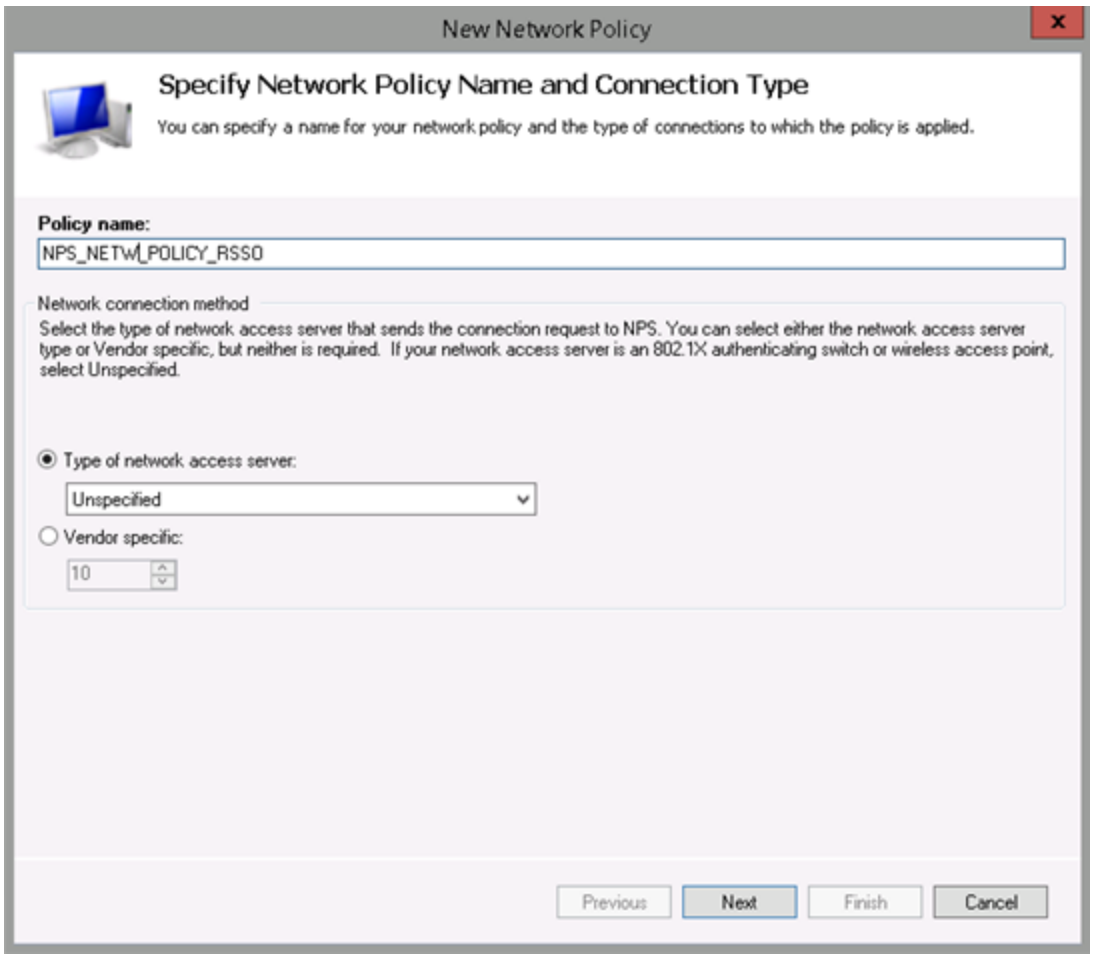


6. On the **Specify Authentication Methods** page, click **Next**.
7. On the **Configure Settings** page, click **Next**.
8. On the **Completing connection Request Policy Wizard** page, click **Finish**.

Network Policy

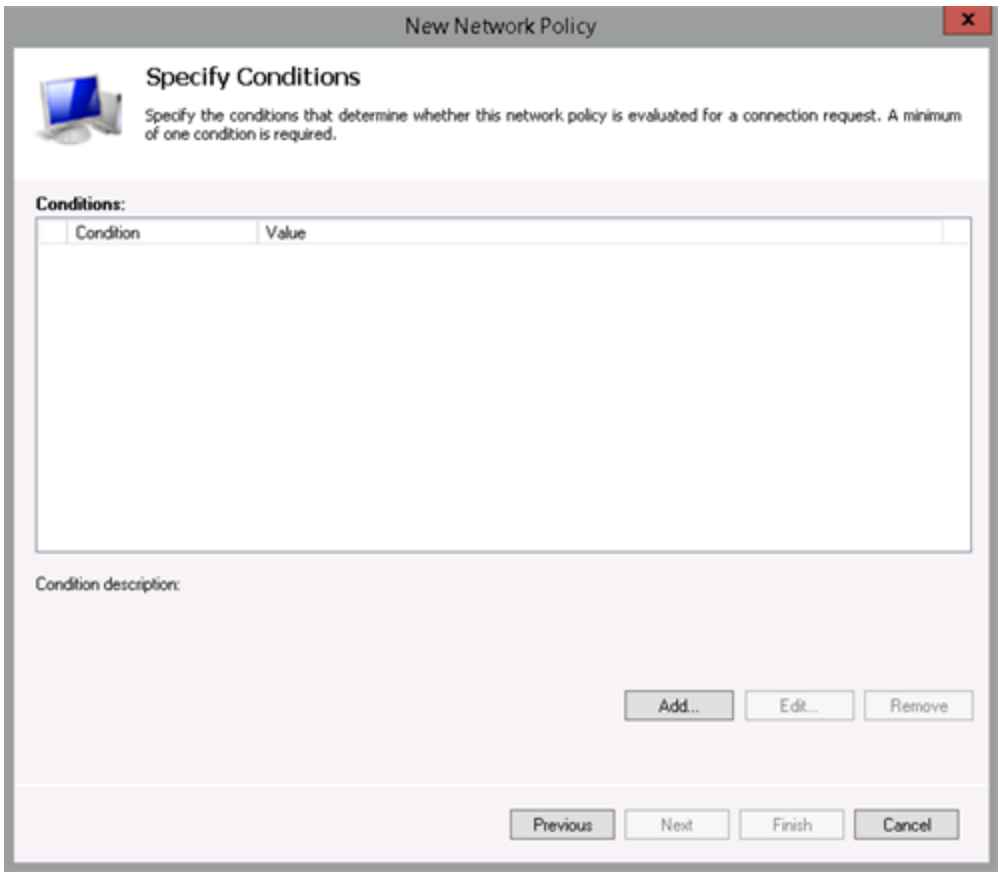
1. In the Network Policy server:
   a. Click on **Policies**.
   b. Right-click **Network Policies**.
   c. Click **New** and provide a Policy Name and click **Next** (make sure to use a descriptive name that will stand out in the Server Security Event Log e.g. *NPS_NETW_POLICY_RSSO*).

Screenshot of NPS Network Policies



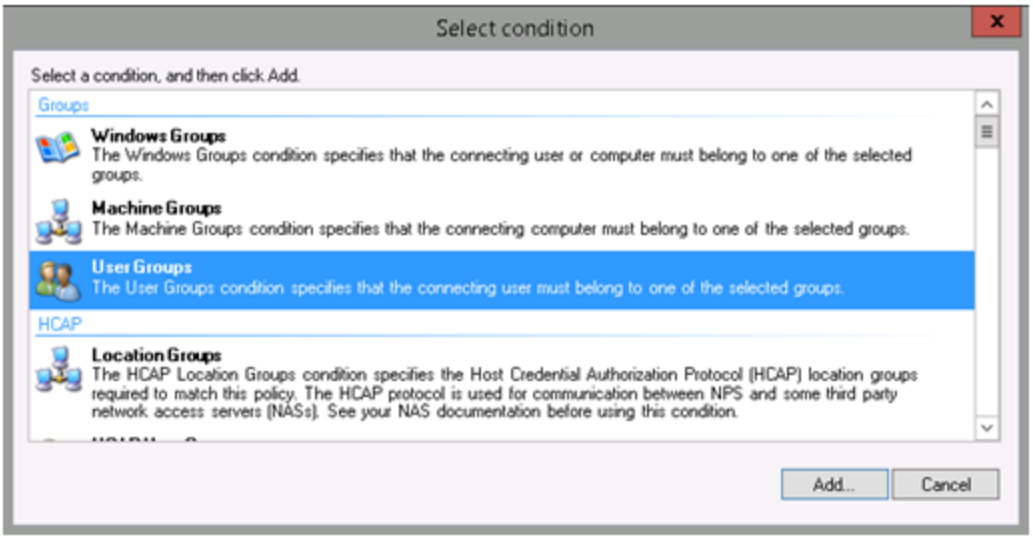
2. In the **Specify Conditions** dialog box, click **Add**.

Screenshot of the Specify Conditions dialog box



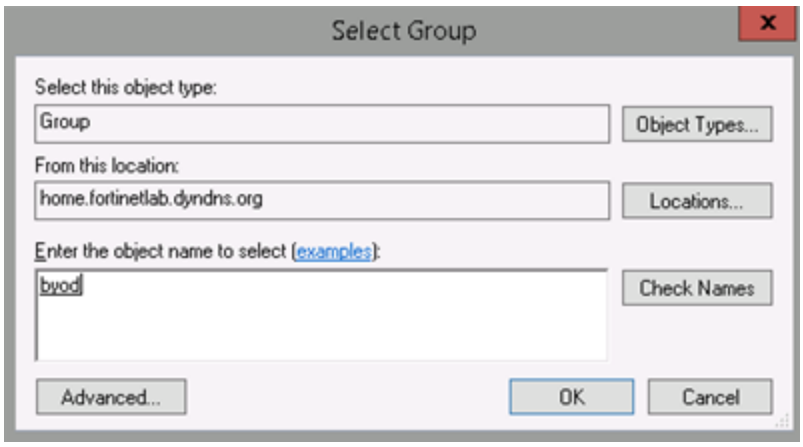
3. In the **Select condition** dialog box, choose **User Groups**, and click **Add**.

Screenshot of the Select condition dialog box



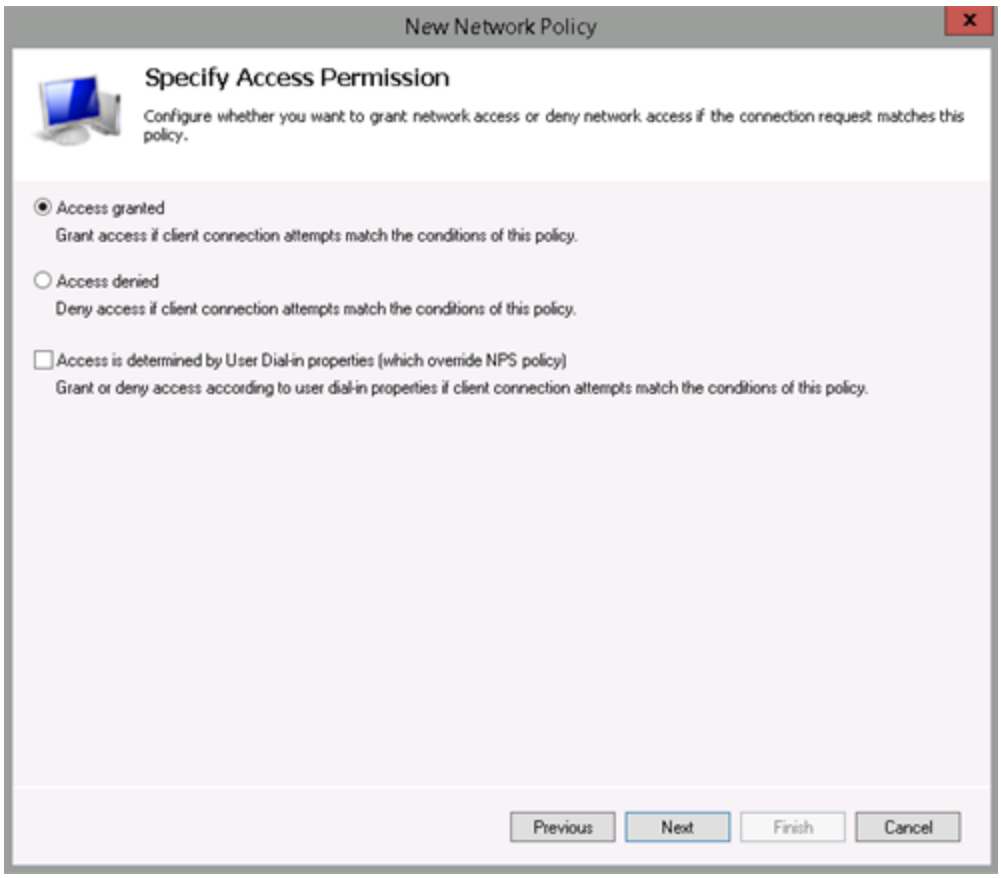
4. Click **Add Groups**.
5. Type in the security group for your BYOD users (i.e. *byod*), click **OK**, and click **OK** again.

Screenshot of the Select Group dialog box



6. Click **Next**.
7. In the **Specify Access Permission** dialog box, select **Access granted**, and click **Next**.

Screenshot of Specify Access Permission dialog box



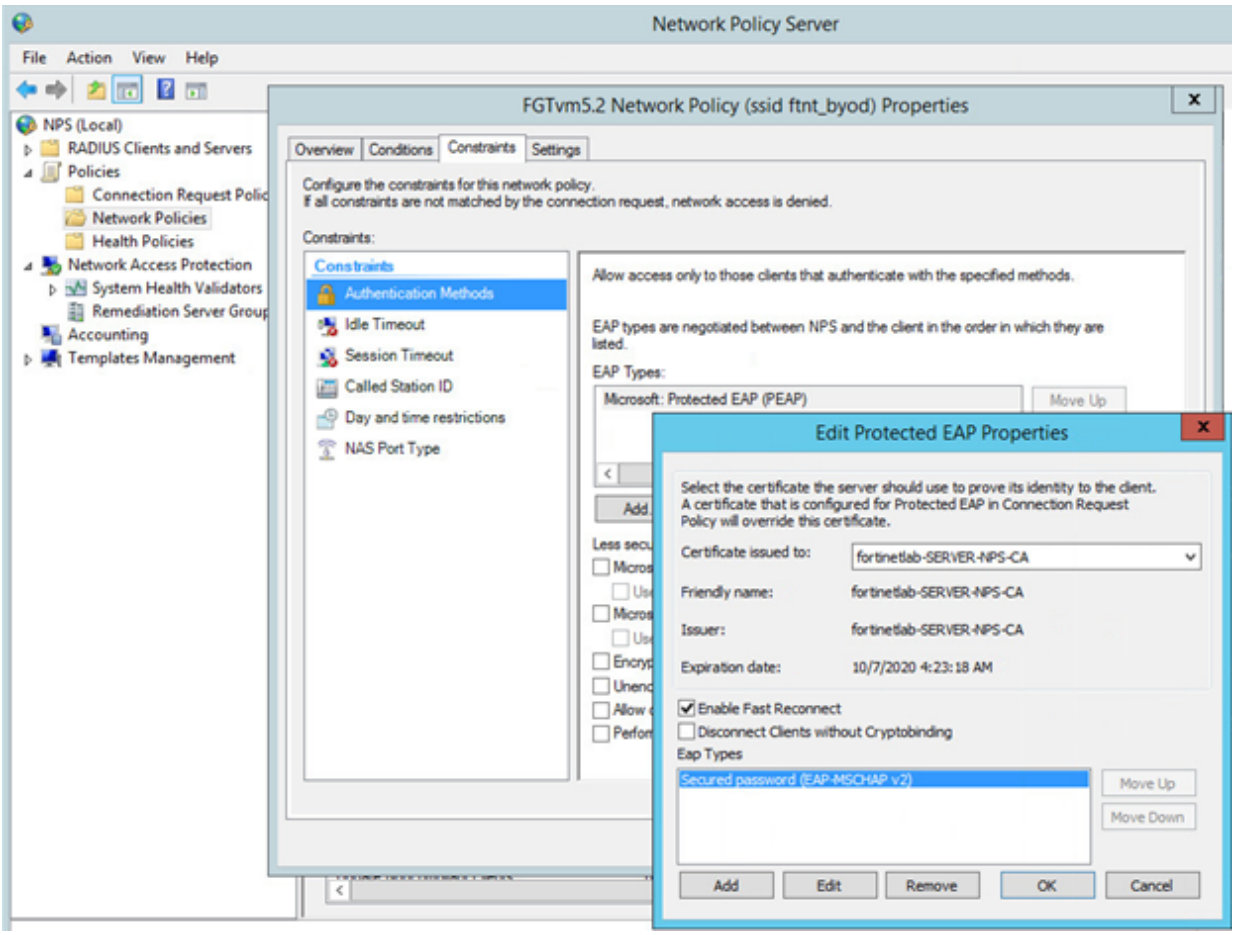
8. In the **Configure Authentication Methods** dialog:
   a. In the EAP Section, click **Add**.
   b. Select **Microsoft: Protected EAP (PEAP)**.

c. Click PEAP to highlight, then **Edit...** (this is where the NPS certificate is linked and is a very important step).

d. Click **OK**.

e. Click **Next**.

Screenshot of Configure Authentication Methods dialog box

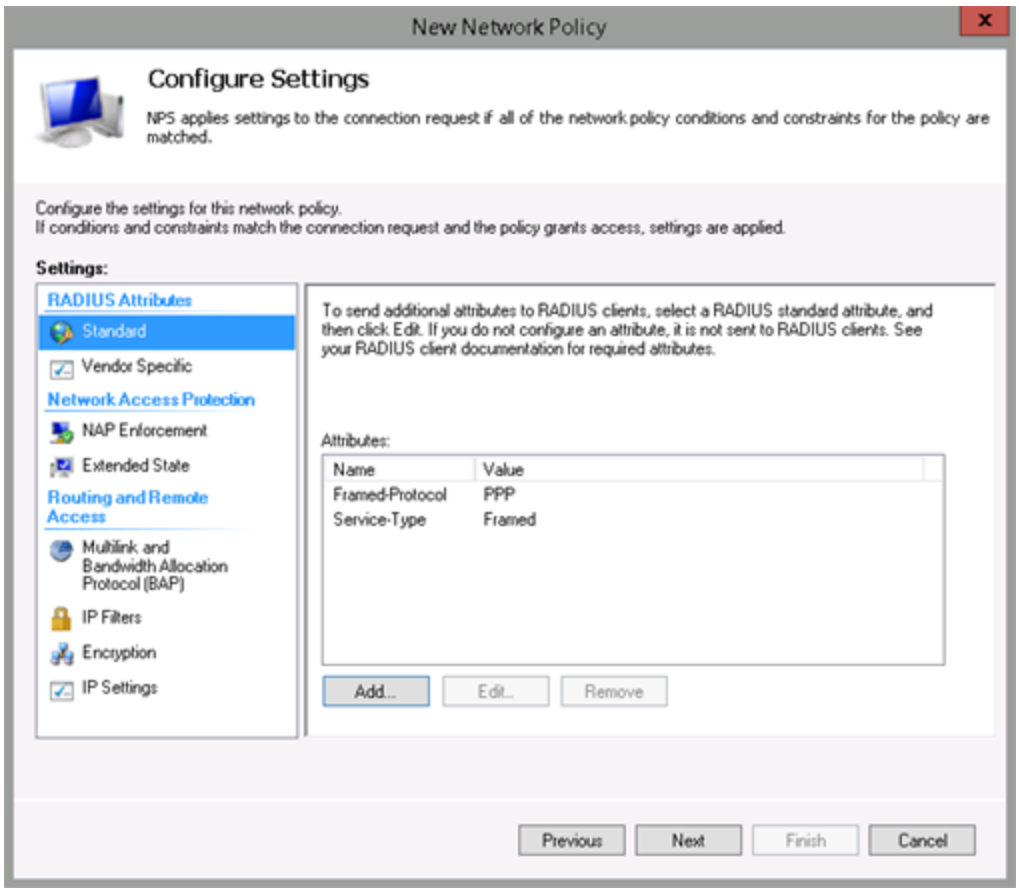


9. In the **Configure Constraints** dialog box, click **Next**.
10. In the **Configure Settings** dialog:

a. Under **RADIUS Attributes**, select **Standard**.

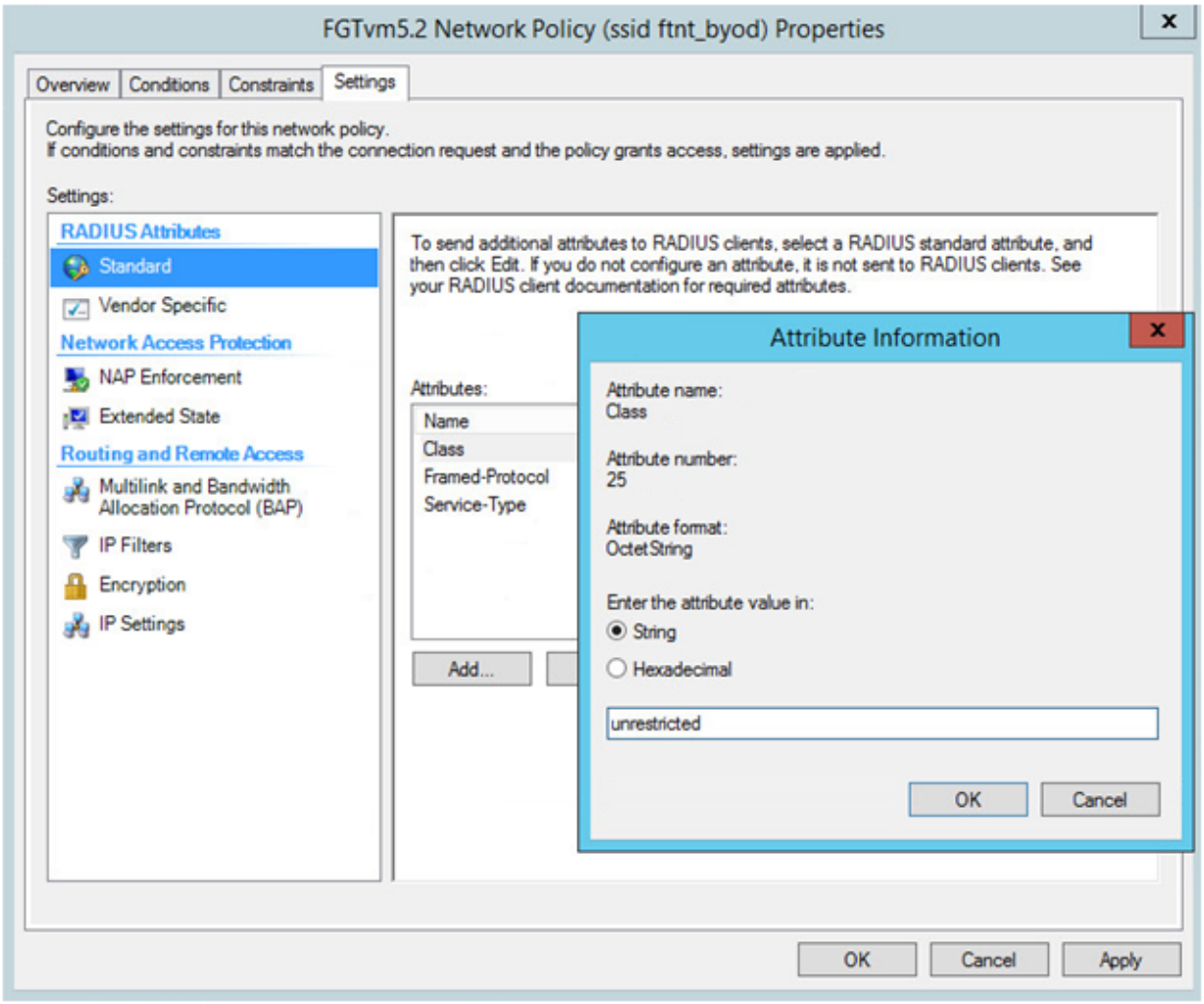
b. Click **Add**.

Screenshot of Configure Settings dialog box



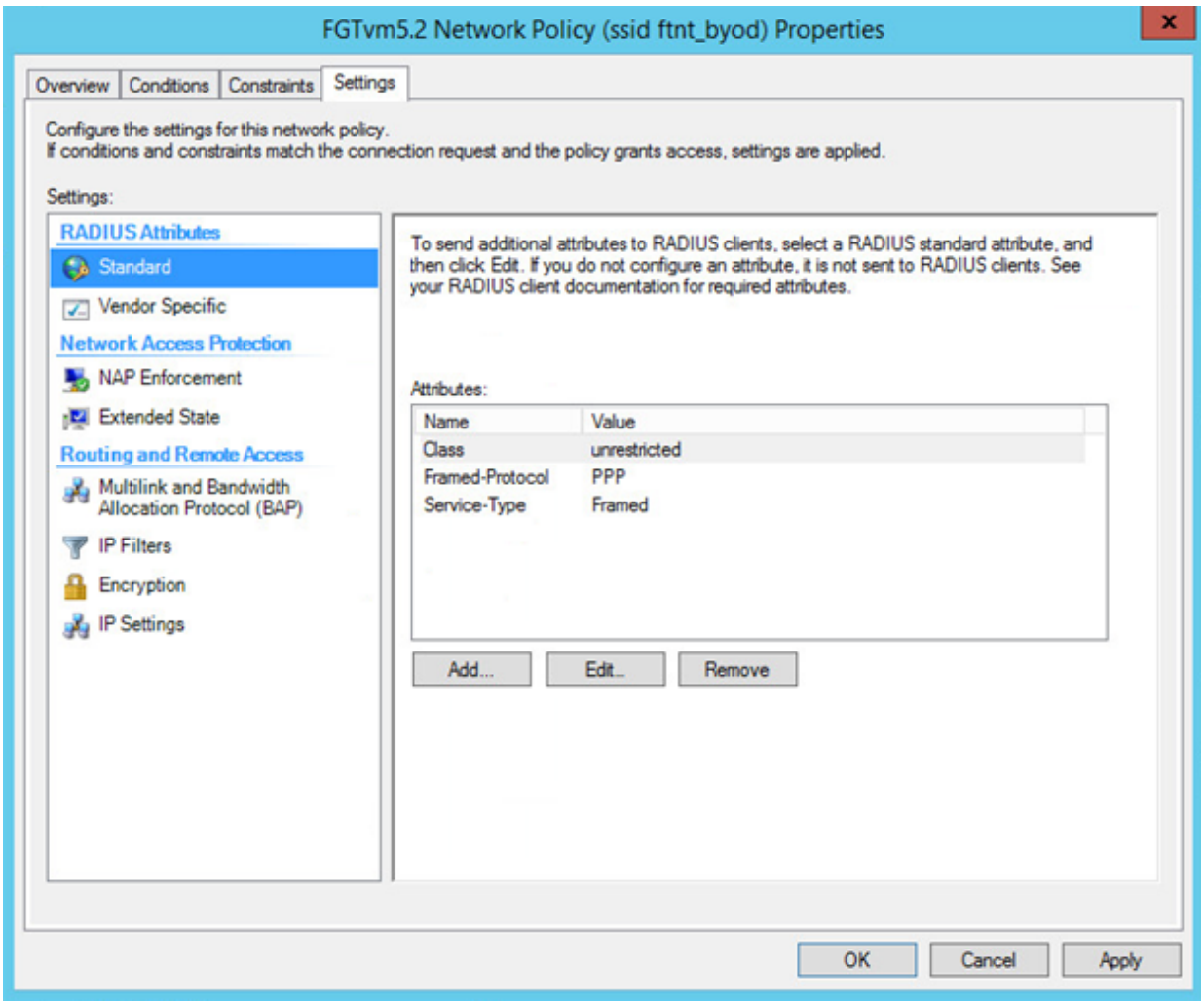
11. In the **Add Standard RADIUS Attribute** dialog:
    a. Select the **Class** attribute.
    b. Click **Add**.
    c. In **Attribute Information** dialog choose **String** and for **Enter the attribute value in** box type the name of the string that will match the value used in the RSSO Group section from earlier.

Screenshot of Add Standard RADIUS Attribute dialog box



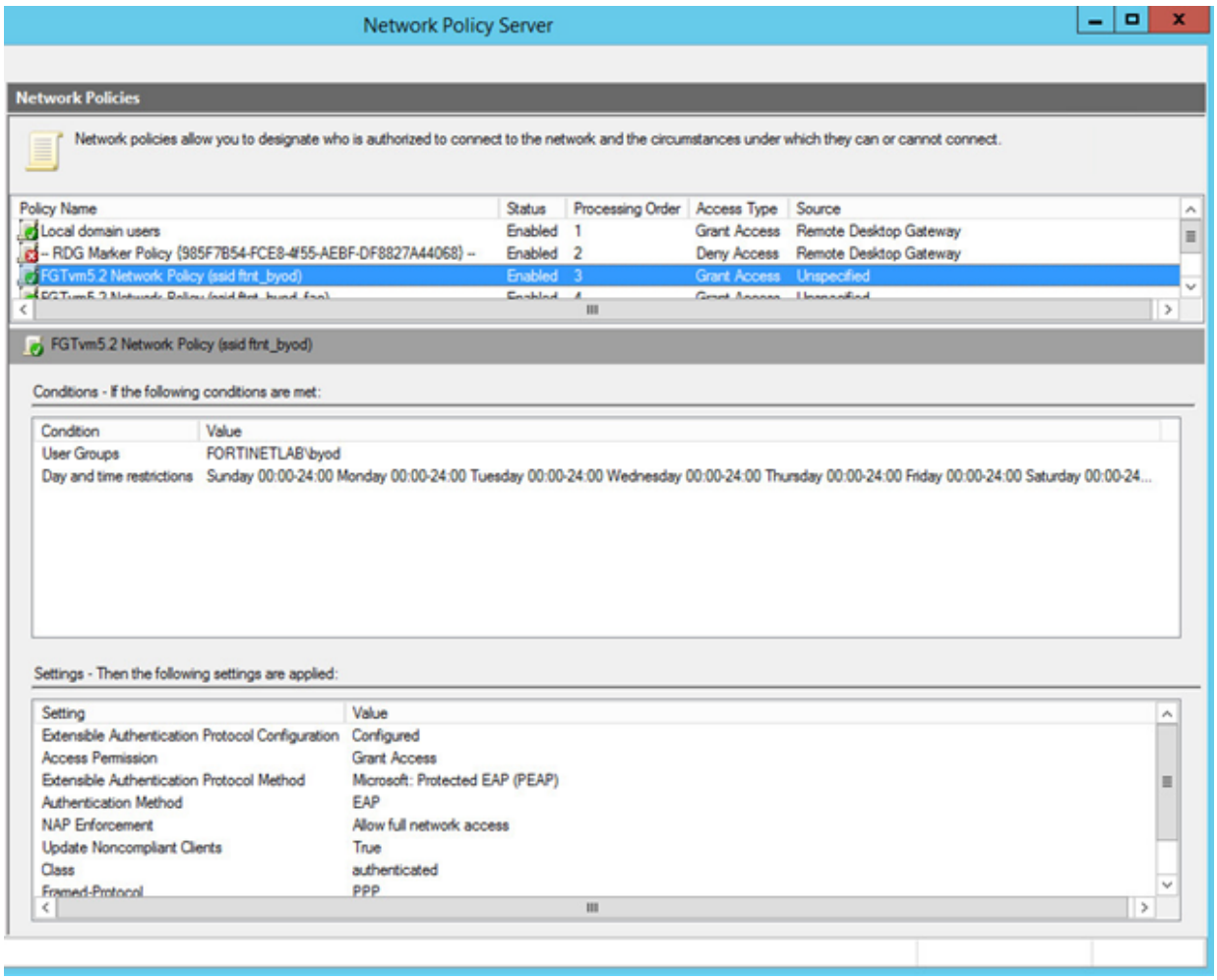
12. Click **OK** and **Close**.
13. Verify the following attributes set.

Screenshot of Configure Settings dialog box



14. Click **Finish** on the **Completing New Network Policy** summary page.

Screenshot of Completing New Network Policy summary

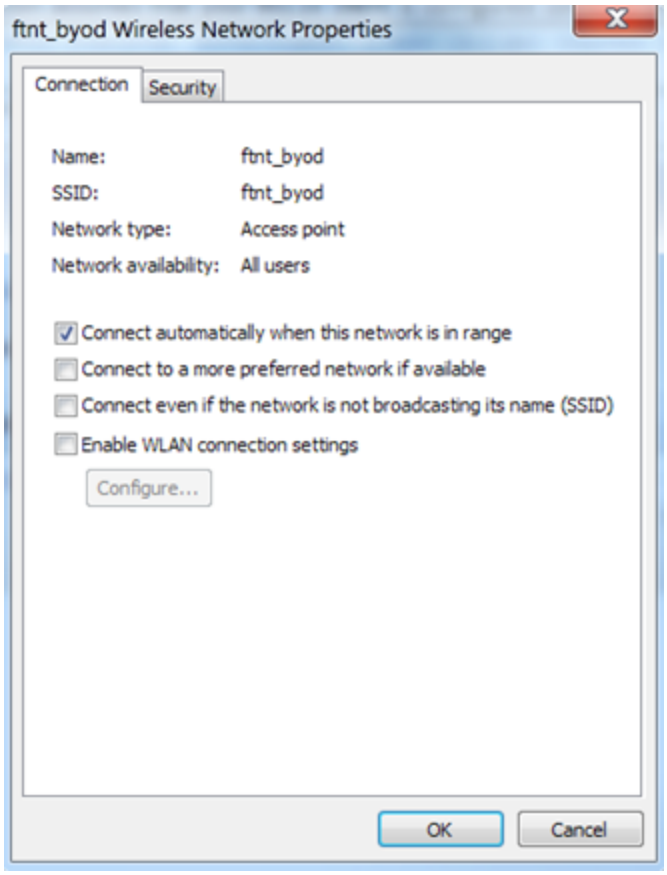


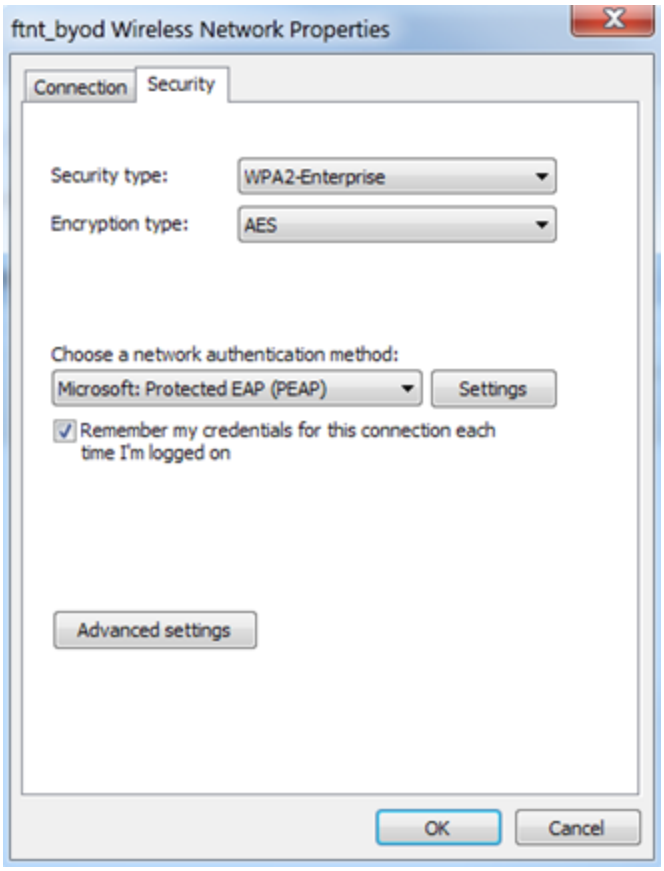
Client Configuration

This section assumes that your 802.1x client is configured correctly in order to connect to an SSID using “WPA2 Enterprise” authentication. A Root CA is also required, but Server Validation is optional.

Below is an example of how the Windows 7 wireless network connection should look on a windows laptop running Window 7 SP1. Add a new wireless connection as shown in the following two images.

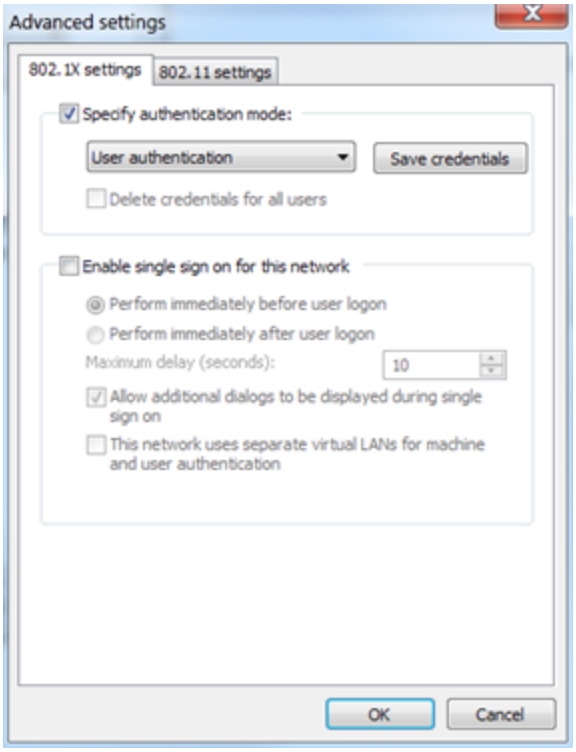
Screenshots of Windows 7 Wireless Properties





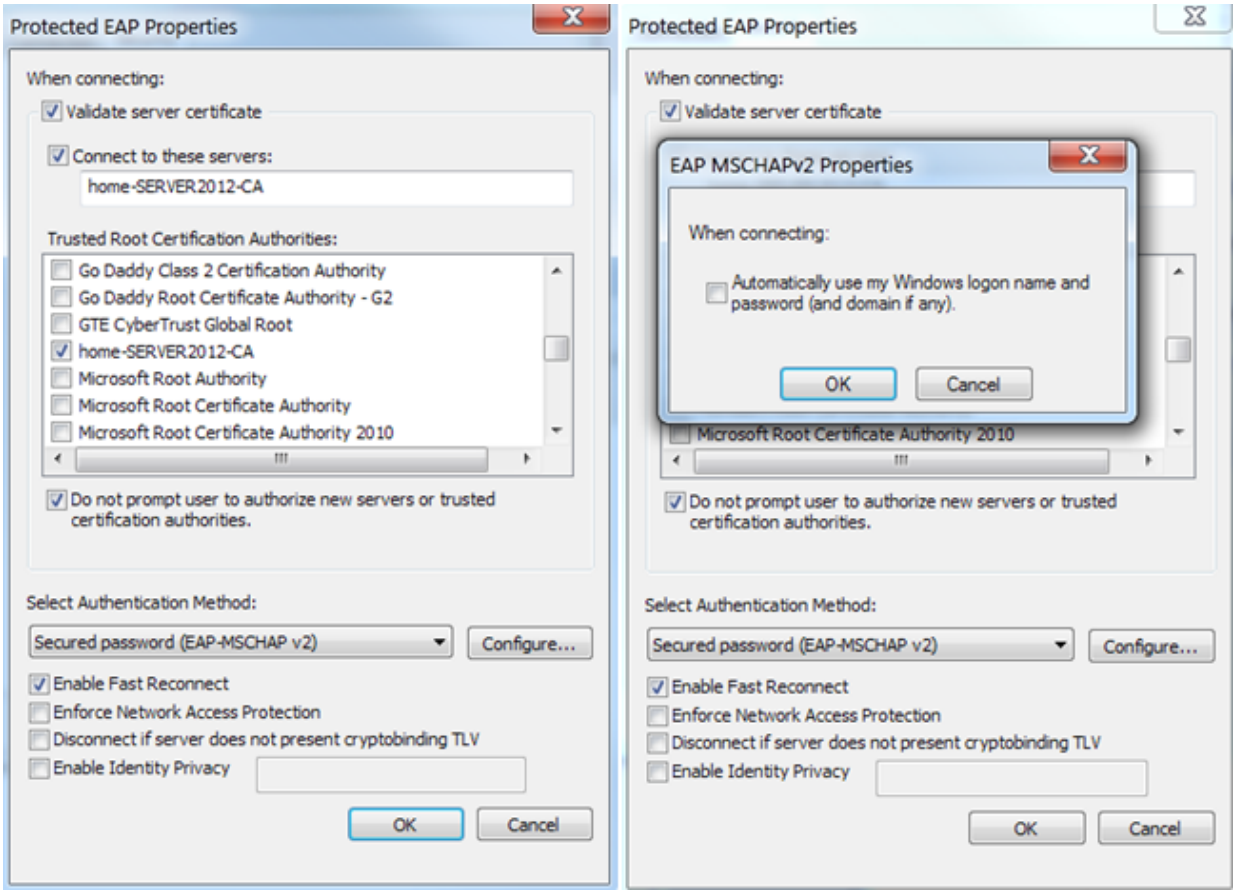
1. Click **Advanced settings**, select **Specify authentication mode**, and select **User authorization**.

Screenshot of Windows 7 Wireless 802.1x Properties



2. Below is an example of Server Validation where the wireless client verifies the certificate it's presented by the NPS server. This step is optional and is one of the most common errors/difficulties when using 802.1x. If **Validate server certificate** is selected then the Root CA certificate from the NPS needs to be added to the Trusted Root Certificate Store of the client. This can be done manually, or by adding Certificate Services Web Enrollment to the NPS server along with an open SSID to allow clients to reach https://192.168.0.1/certsrv to download/install the certificate to the Trusted Root store.
3. Click **Configure...** and make sure that **Automatically use my Windows logon name and password** is not selected. This is also a main source of failure for clients as EAP will try to use the logon name/password of the local machine which is not the same as the users Active Directory credentials.

Screenshots of Windows 7 Wireless EAP



RADIUS Single Sign-On (RSSO) Verification and Testing

To verify correct configuration of these parameters, there are several methods that can be used in combination to validate successful logons via RSSO. Those methods are:

- Firewall CLI debug and packet sniffer commands.
- Traffic analysis using packet sniffer captures and Wireshark.
- Security Event Log on Server 2012 R2.
- Firewall User Monitor and CLI debug commands.

Troubleshooting and Validation Methods

1. Is the WLC forwarding 802.1x and RADIUS traffic to the NPS? Check with a packet sniffer to confirm there is communication between the WLC and NPS.

```
FGTvm-home # diag sniffer packet any 'port 1812 or 1813' 4 500
interfaces=[any]
filters=[port 1812 or 1813]
8.415348 port1 out 192.168.0.1.1030 -> 192.168.10.3.1812: udp 250
8.419272 port1 in 192.168.10.3.1812 -> 192.168.0.1.1030: udp 191
8.444053 port1 out 192.168.0.1.1030 -> 192.168.10.3.1812: udp 288
8.449576 port1 in 192.168.10.3.1812 -> 192.168.0.1.1030: udp 299
8.524302 port1 out 192.168.0.1.1029 -> 192.168.10.3.1813: udp 221
8.526549 port1 in 192.168.10.3.54697 -> 192.168.0.1.1813: udp 231
8.526993 port1 out 192.168.0.1.1813 -> 192.168.10.3.54697: udp 30
8.528827 port1 in 192.168.10.3.1813 -> 192.168.0.1.1029: udp 20
```

2. Further validation is available with a full packet capture which can then be imported to Wireshark. The previous packet sniffer looks like the following which translates into Wireshark. Notice the details including the RADIUS Accounting type (Stop), Username (x120e), Framed IP Address (the DHCP range supplied to clients), the Called Station (the SSID name *ftnt_byod*), and Class attribute (in hex, that equals ASCII 'authenticated').

```
FGTvm-home # diag sniffer packet any 'port 1812 or 1813' 3 500
interfaces=[any]
filters=[port 1812 or 1813]
7.331147 192.168.0.1.1029 -> 192.168.10.3.1813: udp 263
0x0000   0000 0000 0000 000c 2979 8dc6 0800 4500        ........)y....E.
0x0010   0123 f454 0000 4011 fa20 c0a8 0001 c0a8        .#.T..@.........
0x0020   0a03 0405 0715 010f cc50 0410 0107 3cb3        .........P....<.
0x0030   9796 a344 bc55 1d63 9714 83d9 15c0 2c13        ...D.U.c......,.
0x0040   3535 4534 3345 4233 2d30 3030 3041 4537        55E43EB3-0000AE7
0x0050   3628 0600 0000 022d 0600 0000 0101 0778        6(.....-.......x
0x0060   3132 3065 0406 0000 0000 0806 0a00 c802        120e............
0x0070   0506 0000 0000 1e1d 3030 2d30 392d 3046        ........00-09-0F
0x0080   2d42 382d 3336 2d41 323a 6674 6e74 5f62        -B8-36-A2:ftnt_b
0x0090   796f 641f 1345 432d 3535 2d46 392d 4334        yod..EC-55-F9-C4
0x00a0   2d41 322d 3733 3d06 0000 0013 4d18 434f        -A2-73=.....M.CO
0x00b0   4e4e 4543 5420 3131 4d62 7073 2038 3032        NNECT.11Mbps.802
```

```
0x00c0   2e31 3162 1911 4259 4f44 2d75 7365 7273        .11b..authentica
0x00d0   2d68 6f6d 651a 0e00 0030 4417 08ec 55f9        ted00e....0D...U.
0x00e0   c4a2 731a 1800 0030 4418 1246 4150 3231        ..s....0D..FAP21
0x00f0   4233 5531 3330 3030 3137 351a 0c00 0030        B3U13000175....0
0x0100   4419 0655 f6b5 1c2e 0600 0000 782f 0600        D..U........x/..
0x0110   0000 0030 0600 0000 002a 0600 0000 002b        ...0.....*.....+
0x0120   0600 0000 0037 0655 f6b5 9431 0600 0000        .....7.U...1....
0x0130   01
```

```
Radius Protocol
    Code: Accounting-Request (4)
    Packet identifier: 0x10 (16)
    Length: 263
    Authenticator: 3cb39796a344bc551d63971483d915c0
  Attribute Value Pairs
    AVP: l=19 t=Acct-Session-Id(44): 55E43EB3-0000AE76
    AVP: l=6 t=Acct-Status-Type(40): Stop(2)
    AVP: l=6 t=Acct-Authentic(45): RADIUS(1)
    AVP: l=7 t=User-Name(1): x120e
    AVP: l=6 t=NAS-IP-Address(4): 0.0.0.0
    AVP: l=6 t=Framed-IP-Address(8): 10.0.200.2
    AVP: l=6 t=NAS-Port(5): 0
    AVP: l=29 t=Called-Station-Id(30): 00-09-0F-B8-36-A2:ftnt_byod
    AVP: l=19 t=Calling-Station-Id(31): EC-55-F9-C4-A2-73
    AVP: l=6 t=NAS-Port-Type(61): Wireless-802.11(19)
    AVP: l=24 t=Connect-Info(77): CONNECT 11Mbps 802.11b
    AVP: l=17 t=Class(25): 42594f442d75736572732d686f6d65
    AVP: l=14 t=Vendor-Specific(26) v=Fortinet, Inc.(12356)
    AVP: l=24 t=Vendor-Specific(26) v=Fortinet, Inc.(12356)
    AVP: l=12 t=Vendor-Specific(26) v=Fortinet, Inc.(12356)
    AVP: l=6 t=Acct-Session-Time(46): 120
    AVP: l=6 t=Acct-Input-Packets(47): 0
    AVP: l=6 t=Acct-Output-Packets(48): 0
    AVP: l=6 t=Acct-Input-Octets(42): 0
    AVP: l=6 t=Acct-Output-Octets(43): 0
    AVP: l=6 t=Event-Timestamp(55): Sep 14, 2015 21:55:00.000000000 AUS Eastern Standard Time
    AVP: l=6 t=Acct-Terminate-Cause(49): User-Request(1)
```

3. Further validation is available with daig debug commands. Notice similar information to the Wireshark data is seen when monitoring the RADIUS daemon:

```
FGTvm-home # diag debug application radiusd -1
FGTvm-home # diag debug en
FGTvm-home # _event_read[Collector_Agent-1]: received heartbeat 135042
[debug]calling handler[FTNT_BYOD]
[debug]locate_network prhtype(1) pihtype(1)
[note]DHCPINFORM from 10.0.200.2
[note]reply (without ip) to ec:55:f9:c4:a2:73 via FTNT_BYOD(ethernet)
[debug]packet length 300
[debug]op = 1  htype = 1  hlen = 6  hops = 0
[debug]xid = 570923ca  secs = 0  flags = 0
[debug]ciaddr = 10.0.200.2
[debug]yiaddr = 0.0.0.0
[debug]siaddr = 0.0.0.0
[debug]giaddr = 0.0.0.0
[debug]chaddr = ec:55:f9:c4:a2:73
[debug]filename =
```

```
[debug]server_name =
[debug]  host-name = "x120e"
```

4. Futher validation is available with diag firewall commands. Notice that similar information to the Wireshark data and RADIUS daemon is seen when monitoring firewall authentication:

```
FGTvm-home # diag firewall auth list
10.0.200.2, x120e
        type: rsso, id: 0, duration: 200, idled: 0
        group_id: 6
        group_name: BYOD_users
```

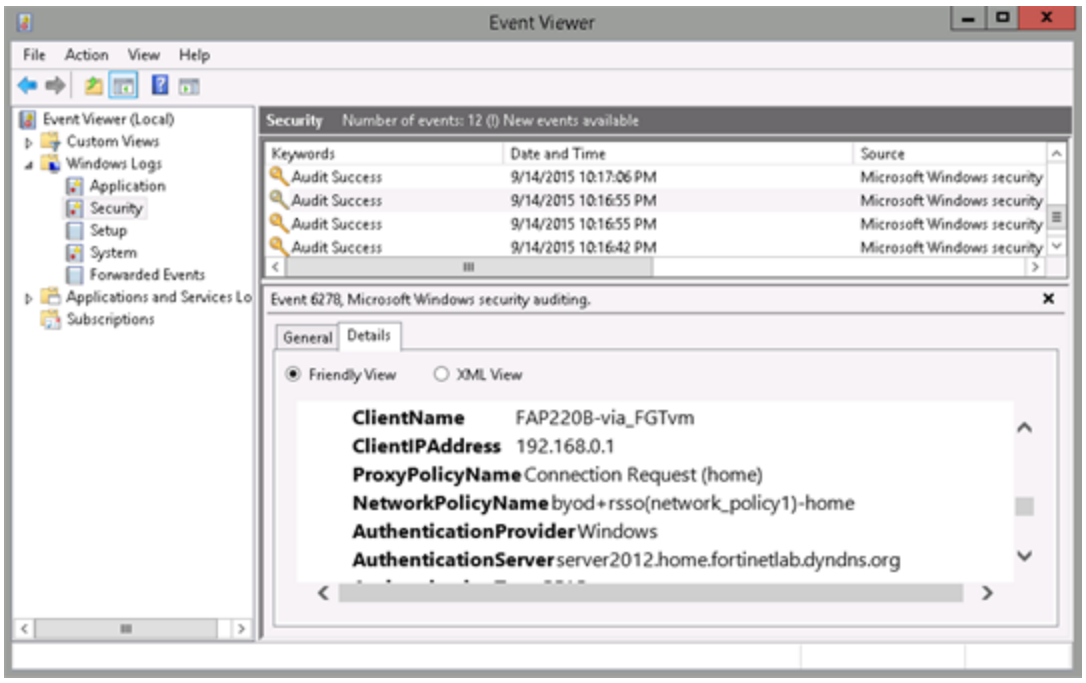
5. Further validation is available with **diag debug application radiusd** CLI commands:

```
FGTvm-home # diag test application radiusd

Radius Daemon Test Usage:
-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-
  2 : Clear RADIUS server database
  3 : Show RADIUS server database
 33 : Show RADIUS server database (with start time)
  4 : Show RADIUS server database info
  9 : Check HA context table checksums
 11 : Show HA sync connection status
 20 : Show RADIUS server configuration cache
 21 : Show RADIUS server interface configuration cache
 99 : Restart
```

6. Further validation is available from the NPS Security Event Log. The usual clues as to why a user cannot authenticate and connect are usually for the following reasons:
   - Is the correct LDAP group being referenced?
   - Is the correct username coming through – remember to not have “Automatically use my Windows logon name and password” selected as shown earlier.
   - If this is being presented during the Windows 7 authentication then Validation Server Certificate was selected but there is no matching Root CA in the Trusted Certificate Store: “The server XYZ presented a valid certificate issued by Company Name Certificate Authority but Company Name Certificate Authority is not configured as a valid trust anchor for this profile”.
   - Is there a matching NPS Connection and Network Policy?
   - Is the correct Authentication and EAP Type selected? (PEAP and MSCHAPv2).

Screenshot of NPS Security Log



7. A final method of validation is available from the Firewall User Monitor which provides a snapshot of the active authentication sessions registered with the FortiGate. To access this in the FortiGate GUI, go to **User & Device > Monitor > Firewall**.